REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)*
15-05-2014

2. REPORT TYPE
FINAL

3. DATES COVERED *(From - To)*

4. TITLE AND SUBTITLE
Overcoming Degraded Communications under A2AD: A Doctrinal Solution

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

LCDR Travis K. Suggs, USN

Paper Advisor: Prof. Patrick Sweeney, Ph.D.& CAPT Andrew Norris, USCG

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
For Example: Distribution Statement A: Approved for public release; Distribution is unlimited. Reference: DOD Directive 5230.24

13. SUPPLEMENTARY NOTES A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

U.S. adversaries are developing Anti-Access/Area Denial (A2AD) strategies that may be utilized against the U.S. in potential conflict. They will seek to apply specific pressure on a U.S. military that is over reliant on communications technology systems, utilizing this as a critical vulnerability to exploit. Currently, our joint force is not fully prepared at the operational or tactical level to assure the attainment of objectives in a degraded or denied communications environment (D2CE). To effectively reorient and protect the warfighting capabilities of our combat forces against A2AD strategies, doctrinal change is required. The joint force, utilizing close coordination between the individual Services, should modify, promulgate and aggressively lead the implementation of new joint and service doctrine that satisfactorily mitigates weaknesses in D2CE operations.

15. SUBJECT TERMS
Joint Operational Access Concept, Joint Doctrine, Asia-Pacific Pivot or Rebalance, C2D2E, EWICE, Contested Environment

16. SECURITY CLASSIFICATION OF:

a. REPORT	b. ABSTRACT	c. THIS PAGE	17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		24	Chairman, JMO Dept

19b. TELEPHONE NUMBER *(include area code)*
401-841-3556

NAVAL WAR COLLEGE
Newport, R.I.

Overcoming Degraded Communications under A2AD: A Doctrinal Solution

by

Travis K. Suggs

LCDR, USN

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: ____________________

15 May 2014

Contents

Paper Abstract

Overcoming Degraded Communications under A2AD: a Doctrinal Solution

U.S. adversaries are developing Anti-Access/Area Denial (A2AD) strategies that may be utilized against the U.S. in potential conflict. They will seek to apply specific pressure on a U.S. military that is over reliant on communications technology systems, utilizing this as a critical vulnerability to exploit. Currently, our joint force is not fully prepared at the operational or tactical level to assure the attainment of objectives in a degraded or denied communications environment (D2CE). To effectively reorient and protect the warfighting capabilities of our combat forces against A2AD strategies, doctrinal change is required. The joint force, utilizing close coordination between the individual Services, should modify, promulgate and aggressively lead the implementation of new joint and service doctrine that satisfactorily mitigates weaknesses in D2CE operations.

INTRODUCTION

The ability to ensure operational access in the future is being challenged—and may well be the most difficult operational challenge U.S. forces will face over the coming decades. – GEN Martin E. Dempsey, Joint Operational Access Concept, January 2012

When one assesses the importance and impact of geopolitical change influencing U.S. military strategy, it is hard to find a time period more critical than early 2012. In relatively rapid succession, the Department of Defense (DoD) released a new Defense Strategic Guidance followed by the Joint Operational Access Concept (JOAC). Defense correspondents and authors of military journals welcomed the increase in clarity at the strategic level, as much confusion and apprehension over the roots of the "Asian Pivot" and the Air-Sea Battle (ASB) concept had become commonplace.[1] The specific emphasis on the Asia-Pacific region and the concern toward Anti-Access/Area Denial (A2AD) strategies were truly watershed moments. It became clear that the joint force had reached a crossroads and embarked on a path that diverged from the low-intensity, large-footprint stability operations of our recent wars in Southwest Asia.[2]

It is now imperative for leaders throughout the joint force to execute a shift in the conceptual framework on how we will undertake military operations against an A2AD challenge.[3] While retaining the counterinsurgency expertise paid for in blood over the last decade, the U.S. military must refine and magnify our proficiency in high-intensity warfare against potentially powerful nation-state adversaries. The JOAC identifies a significant emerging trend that forms the nucleus of our next generation A2AD military problem.

[1] Sam Lagrone, "Pentagon's 'Air-Sea Battle' Plan Explained – Finally", *Wired*, 6 August 2012. http://www.wired.com/2012/08/air-sea-battle-2/.

[2] U.S. Department of Defense, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense (*Arlington, VA: Department of Defense, January 2012), 6.

[3] Paul Johnston, "Doctrine is Not Enough: The Effect of Doctrine on the Behavior of Armies," *Parameters* 30, no. 3 (Autumn, 2000), 30.

Potential adversaries, from regional powers to smaller states, have developed strategies to degrade or deny U.S. technology systems as the most cost-effective way to challenge our qualitative and numerical military advantage. The key problem facing joint commanders will center on conducting operations in a *degraded or denied communications environment* (D2CE). Technological or systems procurement solutions to this challenge will not be satisfactory on their own. Substantive changes to the way we fight can be implemented much more quickly and at a relative cost advantage. Therefore, the joint force should modify, promulgate and aggressively lead the implementation of new joint and service doctrine that satisfactorily mitigates capability deficits in D2CE operations.

DISCUSSION ON THE MOST CAPABLE ADVERSARY: CHINA

A thorough review of potential A2AD strategies that could degrade or deny U.S. military communications technology inevitably leads to a discussion on the People's Republic of China (PRC). Many are reluctant to link A2AD or other emerging warfighting concepts directly with Asia's largest economic and military power. China and the U.S. are intertwined economically and often American foreign policy authors and polemicists are loath to unnecessarily agitate the United States' second largest partner by trade volume.[4] However, an examination of Chinese military capabilities and strategy reveal a military apparatus deliberately designed to exploit perceived U.S. weaknesses.[5] Although future conflict with China is certainly not inevitable, U.S. joint doctrine based on negating the

[4] U.S. Department of Commerce, "Foreign Trade: Top Trading Partners – Dec 2013", December 2013, accessed April 15, 2014, http://www.census.gov/foreign-trade/statistics/highlights/top/top1312yr.html.

[5] Toshi Yoshihara and James R. Holmes, *Red Star Over the Pacific* (Annapolis, MD: Naval Institute Press, 2010), 210.

robust A2AD capabilities the PRC might wield will provide an acceptable strategic counterweight against any alternative adversary.

Chinese strategists are clear on their characterization of a hypothetical conflict with the U.S.: a "local war under high-technology conditions."[6] The PRC understands that to defeat a quantitatively and qualitatively superior foe, a strategy that quickly seizes the initiative by attacking enemy critical vulnerabilities is essential. In the eyes of Chinese strategists, perhaps no possible U.S. military vulnerability is more important than the heavy reliance on its information networks.[7] U.S. conventional forces are especially dependent on space and cyber operations. Units performing joint maneuver and fires require satellite communication datalinks and the ubiquitous global positioning system (GPS) for effective navigation and targeting.[8] Even more readily apparent to any staff supporting a joint force commander is the vast satellite communications (SATCOM) bandwidth requirement to provide intelligence imagery, UAV feeds, and video-teleconferences in support of command and control (C2).[9] Anti-satellite (ASAT) weapons technology offers the PRC multiple avenues for disabling or destroying U.S. space platforms. A space offensive might include kinetic weapons, directed energy weapons, explosive charges, jamming or electronic countermeasures activated in close proximity to U.S. satellite systems.[10] Likewise, computer network attacks (CNA) against the U.S. military are seen as potentially very effective.

[6] Roger Cliff et al., *Entering the Dragon's Lair (*Santa Monica, CA: The RAND Corporation, 2007), xv.
[7] Qingmin Dai, "On Integrating Network Warfare and Electronic Warfare," *Zhongguo Junshi Kexue*, 1 February, 2002, In *FBIS [Foreign Broadcast Information Service] as "Chinese Military's Senior EW Official Explains China's Network Warfare Doctrine,"* June 24, 2002.
[8] David O. Meteyer, *The Art of Peace: Dissuading China from Developing Counter-Space Weapons,* INSS Occasional Paper 60, Colorado Springs, CO: USAF Institute for National Security Studies, 2005, 3.
[9] Ibid.
[10] Pavel Podvig and Hui Zhang, *Russian and Chinese Responses to U.S. Military Plans in Space* (Cambridge, MA: The American Academy of Arts and Sciences), 2008, 57.

Chinese strategists are aware that a vast percentage of U.S. military bandwidth passes through civilian infrastructure and are especially vulnerable to attack.[11]

Some strategists consider that the best way counter China's (or another competitor) interest in employing space and cyber-based threats against US forces is via dissuasion.[12] Not unlike the successful nuclear deterrence strategy of cold war fame, dissuasion would seek to raise the potential risk to Chinese decision makers beyond any possible cyber/space reward if hostilities became imminent. It is essential to note that any current or near-term ASAT, jamming, or CNA capability the PRC may possess can be met or exceeded by the U.S. Even successful PRC attacks against the U.S. military in these domains would very likely result in a non-nuclear version of mutually assured destruction of Chinese space or cyber networks.

However, certain factors would tend to lean this conflict in favor of the PRC via asymmetric advantage. By their nature, U.S. space and cyber capabilities are of most importance supporting forces while in an expeditionary role. But as the most likely center point of US/PRC tension in the near future lies near or in the South China Sea, the Chinese would be far less vulnerable to distance constraints vis a vis the requirement for high-tech communications and satellite capacity. China is continuing investment in hardened and buried closed fiber-optic communications networks that would greatly diminish vulnerability to space and cyber attack.[13] Communications with maritime and air forces in a degraded communications environment would still be quite feasible for a belligerent operating from

[11] Daohai Lu, *Information Operations: Exploring the Seizure of Information Control (*Beijing, People's Republic of China: Junshi Yiwen Press, 1999), 311.

[12] David O. Meteyer, *The Art of Peace: Dissuading China from Developing Counter-Space Weapons,* INSS Occasional Paper 60, Colorado Springs, CO: USAF Institute for National Security Studies, 2005, 76.

[13] van Tol, et al. *AirSea Battle: A Point-of Departure Operational Concept (*Washington, DC: Center for Strategic and Budgetary Assessments, 2010), 19.

interior lines of communication in close proximity to homeland bases and relay stations. PRC forces would be able to fall back on legacy systems such as landline and short to medium-range radio communications. Lack of space and cyber communications capability would serve greatly to handicap an expeditionary force operating far from critical C2 nodes.[14] Therefore, space and cyber warfare during a South China Sea conflict would add a significant asymmetric advantage to China when the factors of space, time and force are evaluated.

The likelihood of facing these types of warfare forms the root of our peacetime challenge in reorienting the force to maintain U.S. combat dominance. Failure to address D2CE might create a series of faulty assumptions regarding U.S. combat effectiveness against an adversary employing these high-tech A2AD strategies. Faulty assumptions will result in faulty operational planning.[15] Therefore, the challenges of operating without our accustomed degree of communications technology is a problem that lies squarely at the operational level.

MAIN ARGUMENT: DOCTRINE TO OPERATE UNDER D2CE IS INSUFFICIENT

"The U. S. Navy and its coalition partners recognized that maritime doctrine, organization and training are not optimized to support operations in an environment in which command and control is denied or degraded," - RADM Terry B. Kraft, commander, NWDC

It is a repetitive feature in military history that a nation state is often drawn toward the tendency to train to fight as they did in previous conflicts – a concept often called the "last

[14] Paul D. Berg, U.S.A.F, "Expeditionary Operations," *Air & Space Power Journal* 22, no. 2 (Summer, 2008), 29, http://search.proquest.com/docview/217769894?accountid=322, Accessed April 12, 2014.

[15] David A. Rickards, "No Air: Cyber Dependency and the Doctrine Gap" (research paper, U.S. Naval War College, Joint Military Operations Department, Newport, RI, 2010),.9.

war syndrome."[16] The Joint Force is slowly recovering from nearly a decade of combat operations in Iraq and Afghanistan. We now carry with us invaluable new lessons paid for in blood and treasure concerning counterinsurgency and stability operations. But we may also be returning with overdependence on high-bandwidth communication systems and the contractors required to maintain them.[17]

The U.S. military in its entirety or by its individual services is of course, a human institution. Our service cultures place an extraordinarily strong value on leadership and the passing of experience from senior officers and NCOs to the next generation of warfighters. The shared experiences of today's best and most seasoned operators add massive value into our combat effectiveness, but cannot be expected to apply to the full range of future conflicts. Shaping how our warfighters counter high-technology threats applies directly to the emphasis the JOAC places on the increased capabilities of tomorrow's potential enemies.[18] High-intensity warfare experiences against a comparable opponent or in a contested communications environment are no longer easily drawn from the collective memories of each service as these types of conflict occurred generations ago. How can we minimize this void? The services must ensure the ability to reach back for lessons learned from our forebears in order to fill seams and gaps that might exist in our ability to conduct conventional warfare under degraded technology conditions.[19]

[16] John D. Waghelstein, "Military-to-Military Contacts: Personal Observations – The El Salvador Case" (Fall 2002), 12. Quoted in Frank Cass, *Low Intensity Conflict and Law Enforcement* (London Vol. 10, No2, Summer 2003).
[17] Stew Magnuson, "U.S. Forces Prepare For a Day Without Space," *National Defense Magazine* (February 2014), http://www.nationaldefensemagazine.org/archive/2014/February/pages/USForcesPreparefora%E2%80%98DayWithoutSpace%E2%80%99.aspx
[18] U.S. Department of Defense, *Joint Operational Access Concept, Version 1.0* (Arlington, VA: Department of Defense, January 2012), ii.
[19] David Fitzgerald, *Learning to Forget: US Army Counterinsurgency Doctrine and Practice from Vietnam to Iraq* (Stanford, CA: Stanford University Press, 2013), 134.

The JOAC clearly captures the JCS Chairman's recognition of the challenges emerging in the space and cyber domains. Multiple capability requirements are identified and grouped according to the various joint functions to support the successful implementation of a successful D2CE warfighting concept. Right from the start, the authors identify the need for "effective command and control in a degraded and/or austere communications environment."[20] But beyond this opening acknowledgement of the importance of executing C2 under degraded conditions, clear emphasis on the concept begins to fade. While joint intelligence functional capabilities imply the ability to deliver intelligence products to the joint force under "opposed access situations," under no other joint functions are degraded communications challenges specifically highlighted.[21]

SUPPORT #1: D2CE DOCTRINE MUST APPLY TO ALL OPERATIONAL FUNCTIONS

The singular emphasis on command and control to the detriment of the other operational functions is the central deficiency in our existing joint and service doctrine with respect to C2DE. For example, the Navy's WDC (Warfare Development Command) has recognized the challenges associated with operations in a denied or degraded communications environment, and in response published a 2012 TACMEMO attempting to address the competency shortfall. It specifically identifies capability gaps regarding operations in a potential stressed-communications situation. The preferred acronym used by the WDC to describe the challenge is C2D2E (Command and Control in a Degraded or

[20] U.S. Department of Defense, *Joint Operational Access Concept, Version 1.0* (Arlington, VA: Department of Defense, January 2012), 34. This is promptly listed as capability JOA-002 in the Command and Control function listing.
[21] Ibid.

Denied Environment). Although this is in alignment with the JOAC, it is essential that Navy doctrine apply not just to the command and control function but to all operational functions required of naval forces.

To illustrate, note the most recently released Required Operational Capabilities/Projected Operational Environment (ROC/POE) for the USS Blue Ridge (LCC-19):

> Denial or degradation of satellite and or network dependent C2 systems will require use of legacy systems such as tactical signals, line–of-sight radio communications and celestial navigation (among others) to ensure continuity of C2 capabilities. Personnel capable of operating the aforementioned legacy systems are frequently not present in Navy ships… Accordingly, all assigned personnel having duties involving C2 (both ship's company and personnel assigned to embarked staffs) shall attend the C2D2E training… appropriate to their respective positions when that training becomes available.[22]

As it is the command ship of the Japan-based U.S. 7th Fleet, it is suitable that the Blue Ridge appears to be leading the fleet in the acknowledgement of and the initial steps to counter the D2CE challenge. However, the deficits mentioned in trained personnel (or a currently active training program) likely will apply beyond just C2 capabilities.

The spillover effects experienced while experiencing denied communications could affect every functional aspect of the military apparatus. Each service implementing their responses to the challenge might very well succeed in fostering the JOAC's "cross-domain synergy" C2 concept but fail to have adequately prepared units who are struggling to navigate to objectives, acquire precise timing for maneuver and ensure the accuracy of munitions delivery in a denied communications environment.[23] As weapons direction and navigation equipment are often as reliant on satellite and cyber as command and control

[22] U.S. Office of the Chief of Naval Operations, *Required Operational Capabilities and Projected Operational Environment for Amphibious Command Ship (LCC-19) Blue Ridge*, OPNAV Instruction 3501.33F (Washington D.C.: DON, 8 May 2013), 4.

[23] U.S. Department of Defense, *Joint Operational Access Concept, Version 1.0* (Arlington, VA: Department of Defense, January 2012), ii.

systems, the D2CE problem directly affects joint fires and movement and maneuver. Logistics and sustainment movements will be slower and less coordinated as strategic lift assets over air and sea share the same navigational reliance on satellite and cyber systems as combat ships and aircraft.[24] Intelligence functions would be drastically curtailed. Emphasis on command and control is necessary but not sufficient enough on its own. Joint and individual service doctrine must direct the expansion of D2CE capabilities beyond C2 cross-domain synergy to underpin the entire spectrum of joint functions required at the operational level.

Despite the functional shortcomings, the Navy WDC TACMEMO remains a step in the right direction that translates the D2CE guidance of the JOAC into an operative service directive. However, the WDC acknowledges that the TACMEMO is designed to fill gaps in Navy doctrine, organization and training.[25] The importance of this issue demands that the WDC develop an unclassified Naval Warfare Publication (NWP) directly establishing D2CE doctrine from the ground up, Navy-wide. Instead of filling gaps, a sweeping NWP document would expose the D2CE concept to the widest possible audience within Navy operational and training communities and at the earliest opportunity for our newest generation of officers and sailors. The addressees would include all activities of Naval Education and Training Command, as well as more advanced weapons and tactics schools.

Perhaps unsurprisingly, the USAF has also taken a keen interest toward the challenges of maintaining combat superiority during high-intensity conflict. Air Force service culture has often focused heavily on high-tech warfighting in a conventional war

[24] James Drew, "House Subcommittee Hears of Chinese Threats to U.S. Space Assets," *Inside Missile Defense* vol. 20, no. 3 (Feb 05, 2014), http://search.proquest.com/docview/1494380793?accountid=322., Accessed April 10, 2014.

[25] Navy Warfare Development Command Public Affairs, “Navy Warfare Development Command Releases Tactical Memorandum”, accessed April 10, 2014, http://www.navy.mil/submit/display.asp?story_id=67733.

amongst nation-states, often to the criticism of senior DoD officials or other services.[26] However, the Air Force has already taken some initial concrete steps to address the challenges of a degraded or denied communications scenario. Unexceptionally titled "Readiness Project-2," the USAF Air Combat Command (ACC) has embarked on a program designed to change the way the service trains to fight.[27] In remarks made to the 2013 Air Force Association Air and Space Conference, ACC Commander Gen Mike Hostage noted:

> The certainty of our communication links, our pervasive datalinks, our far-seeing radars, and incredibly accurate GPS systems have bred generations of aviators who know little of the old-school TTPs of chattermark, no-radar procedures, and counter-radar jamming. As we exercised our incredible capabilities since the onset of Desert Storm, our adversaries have taken careful note and have been investing in asymmetric ways to deny us these systems.[28]

The Air Force often refers to these endeavors as "operations in a contested environment."[29] Subsequently, a combined USAF and defense industry study was initiated to explore the concept of Effective Warfighting in Contested Environments (EWICE). The Air Force appears focused on the challenge and has advanced the development of service doctrine to maintain their combat capacities under D2CE. However, the service should remain wary to avoid stovepiping innovative approaches, best-practices and lessons learned into service-only lanes.

[26] John A. Tripak, "Gates Versus the Air Force," *Air Force Magazine*, Vol. 97, No. 3 (2014), http://www.airforcemag.com/Features/Pages/2014/box020514gates.aspx.
[27] Sydney J. Freedberg Jr., "Air Force Seeks Quick Fixes to Combat Chinese Electronic Attacks," *Breaking Defense*, September 18, 2012, http://breakingdefense.com/2012/09/air-force-seeks-quick-fixes-to-combat-chinese-electronic-attacks/.
[28] Gen Gilmary M. Hostage, Opening Address, Air Force Association 2013 Air & Space Conference and Technology Exposition, Washington D.C., 17 September, 2013.
[29] Lt Gen William J. Rew, Moderator's Comments, EAST Joint Warfighting Conference '13, Virginia Beach, VA, 14 May, 2013.

SUPPORT #2: DOCTRINAL CHANGE NEEDED TO SHAPE OUR ENTRY-LEVEL WARFIGHTERS

Each year, tens of thousands of new officers and enlisted recruits join our military and naval services. Every one of them has matured under an information technology revolution every bit as important in its impact to American society as the industrial revolution that preceded it. Today's generation of service members is drawn from what is often labeled the Millennial Generation.[30] The profound expertise and agility with technology that these new Millennials will offer when they don the uniform very much interests the current generation of military leaders. However, there is a grave concern about our combat effectiveness when and if our newest generation of warfighters is thrust into a D2CE environment. Now more than ever, military leaders must devote careful study as to exactly what our younger generation of operators at the tactical level *expects* and *requires* in terms of communications tech systems on the battlefield.[31]

Properly assembled, disseminated and implemented by leaders, doctrine can effect change to how our junior warfighters approach the employment of their combat systems. Once clearly promulgated by CJCS and the services, putting D2CE warfighting doctrine into practice will become the final, most difficult, and most important step. To alter the high-tech communications zeitgeist that permeates the tactical units of our military will take direct on-scene leadership. Operational and tactical-level commanding officers will be required to provide the breathing space necessary for effective training under D2CE doctrine. They will require increased planning for risk-management to ensure safety for ships, squadrons or

[30] Neil Howe and William Strauss, *Millennials Rising: the Next Great Generation* (New York, NY: Vintage Books, 2000), 37.
[31] Lt Gen William J. Rew, Moderator's Comments, EAST Joint Warfighting Conference '13, Virginia Beach, VA, 14 May, 2013.

battalions operating under extended periods of time under actual or simulated degraded conditions. Those attempting to reform the way we fight may have the difficult task of separating recent warfighting experiences of a fully assured, tech-reliant environment from the peacetime innovation required to operate under D2CE.[32]

Task force or other operational commanders should provide their subordinate units opportunity for self-contained, ungraded exercises where D2CE doctrine can be translated into warfighting proficiency. This tactical-level training would ideally occur well before operational level exercises such as a Joint Task Force Exercise (JTFX). Unit commanders must restrain the dreaded zero-defect impulse to allow initial mistakes in training under degraded conditions to be made while applying doctrine to unit-specific techniques, tactics and procedures (TTPs). Only then can units experiment, evaluate, and promulgate changes needed to satisfy the operational requirements. Channeling the creative energies of our junior warfighters will provide the spark that will enable our joint force to achieve the capabilities required of the JOAC.

ALTERNATIVE VIEWS TO A DOCTRINAL APPROACH AND REBUTTAL

It may be argued that the vulnerabilities inherent in DoD satellite or cyber communications systems can be mitigated through defense acquisitions. Over time, space and cyber defense technology commensurate with the threat can be expected to develop. However, in the near term, budgetary planning uncertainties and funding for future combat systems are issues that will hamper efforts to design and acquire technological fixes to the

[32] Paul Johnston, "Doctrine is Not Enough: The Effect of Doctrine on the Behavior of Armies," *Parameters* 30, no. 3 (Autumn, 2000), 39.

issue.[33] The Air Force, as well as the Navy, has investigated training simulators as a possible cost-effective approach, although questions remain about their effectiveness in relation to their additional cost.[34] To confront the problem now, Air Force units are experimenting with degraded systems familiarization using techniques as simple as switching GPS off during training. Such rudimentary methods may seem trivial, but they strike at the heart of the problem. Overreliance on communications technology can only be countered by investment in additional training time and resources. Our pilots, shiphandlers, and systems operators can then become familiarized with the D2CE challenge and improve their comfort and effectiveness while working under stressed conditions. Joint and service doctrines clearly establishing the value of this training will be essential in an austere fiscal environment for military budgets.

Some might also argue that adequate steps are being taken to prepare the joint force through operational exercises and wargaming. Joint task force commanders are able to tailor scenarios to simulate D2CE conditions in order to provide participating units some level of exposure to the contested communications challenge. Navy Warfare Development Command's Bold Alligator series of amphibious assault exercises are one example.[35] In this exercise, Expeditionary Strike Group TWO (ESG-2) provided a platform for interaction between fleet assets and WDC observers attempting to grapple with degraded command and

[33] Sydney J. Freedberg Jr., "Air Force Seeks Quick Fixes to Combat Chinese Electronic Attacks," *Breaking Defense*, September 18, 2012, http://breakingdefense.com/2012/09/air-force-seeks-quick-fixes-to-combat-chinese-electronic-attacks/.
[34] Joint Lessons Learned System, "C2D2E Solutions and Recommendations Input", accessed through JLLS (restricted) on April 10, 2014.
[35] Navy Warfare Development Command, "Navy Warfare Development Command 2012 Bold Alligator Fact Sheet", accessed April 10, 2014, www.public.**navy**.mil/usff/ba/documents/ba12_info.pdf.

control challenges.[36] Recently, the Naval War College has sponsored the 2013 Global War Game, exploring combined C2 structures while executing simulated cross-domain operations in a high-intensity A2/AD environment.[37]

Can exercises and wargames alone comprise a sufficient catalyst to change effectively how the Navy (or the other services) fights? These examples are of excellent benefit to D2CE problem-solving efforts that are already underway, but they cannot shoulder the entire burden to assure D2CE expertise alone. Operational level exercises should be devised to evaluate the finished product. They should validate warfighting capability under challenging degraded conditions for tactical units already well prepared from initial training and workup periods. At most, exercises should identify the few TTP shortfalls that can be corrected by units at sea or in the field at peak readiness. In other words, sound joint and service doctrine should drive superior exercise performance. Operational exercises should not drive new doctrine. Exercises by themselves are too infrequent, expensive and evaluation-driven to provide a platform for the joint force to build and refine the capability to operate with degraded communications. These exercises are often documented through exclusively classified reporting systems, restricting the dialogue of lessons learned or doctrinal requirements to be received by service training commands that operate almost wholly in unclassified channels.

[36] U.S. Federal News Service, LLC, "Navy Warfare Development Command Releases Tactical Memorandum." *US Fed News Service, Including US State News*, Jun 12, 2012, http://search.proquest.com/docview/1019843532?accountid=322, accessed April 15, 2014
[37] Briefing, U.S. Naval War College, subject: Global 2013 Game Report, 11 March 2014, E-1.

CONCLUSION

The “pivot” or “rebalancing” to the Asia-Pacific region will require more than a geographic shift.[38] Our forces must also rebalance our focus on how we will conduct future combat operations to the realities of what our next adversary might bring to the fight. The innovative concepts emphasized by the JOAC are welcome guidance from strategic leaders that understand the importance of adapting to the uniquely challenging capabilities of tomorrow’s military threats. The most important implication in the JOAC (and for that matter, AirSea Battle) is that joint and service leadership must be able to translate these operational concepts into an effective doctrinal framework.

The National Command Authority, as well as the geographic combatant commanders, clearly expects that joint commanders at the operational level can utilize effective command and control under D2CE. Cross-domain synergy is at the heart of the C2 solution that is enthusiastically promoted in the JOAC. But we cannot neglect to prepare our ships, squadrons and battalions in carrying out all other operational functions as well. Joint force commanders will presume that when units are directed to maneuver and employ fires, those units can do so facing D2CE conditions. We cannot accept the risk that this core operational assumption might be proven incorrect should our military face the full weight of the A2AD challenge that seeks to capitalize on our critical vulnerabilities. Central to this task is to ensure that there is no shortfall in doctrine that enables our warfighters to get the job done even without GPS, SATCOM or other communications technology. Professor Milan Vego of the Naval War College noted in a routine lecture on operational art that the “focus should always remain on leadership and warfighting” in contrast to technology or systems-driven

[38] U.S. Department of Defense, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense (*Arlington, VA: Department of Defense, January 2012), 6.

approaches to winning military conflicts.[39] Preparing for future warfare in accordance with the JOAC means we cannot expect the unlimited communications technology we've become accustomed to. It will require that we capitalize on the initiative and ingenuity of our people, the doctrine to guide them and the leadership to energize both.

RECOMMENDATIONS

Promulgate a single joint term to describe the concept. The U.S. Navy currently uses the term Command and Control in Degraded or Denied Environment (C2D2E) in its description of the problem. The U.S. Air Force often describes the concept as Operations in a Contested Environment, or Effective Warfighting in a Contested Environment (EWICE). C2D2E restricts the scope of the problem by implying a solution via only one of the operational functions: command and control. EWICE is sufficiently broad, but does not clearly describe in detail exactly what the contested domains are. Recommend that CJCS adopt the phrase Degraded or Denied Communications Environment (D2CE) into the joint terminology lexicon. This term sufficiently defines the nature of the challenge and is broad enough to cover each joint operational function.

Modify the Joint Operational Access Concept (JOAC) to direct support of D2CE capabilities throughout all operational functions. Required command and control capability JOA-002, as promulgated in the JOAC, specifically prioritizes "the ability to perform effective command and control in a degraded and/or austere communications environment."[40] However, this

[39] Prof. Milan Vego, "Introduction to Maritime Warfare Theory" (lecture, U.S. Naval War College, Newport, VA, 10 March 2014).

[40] U.S. Department of Defense, *Joint Operational Access Concept, Version 1.0* (Arlington, VA: Department of Defense, January 2012), 34.

capability is not specifically restated in any of the other joint operational functions. Dependence on communications technology is a potential critical vulnerability throughout all functional components of the joint force. Joint and service leadership should effectively direct the Joint Capabilities Integration Development System (JCIDS) process to address any D2CE capability caps throughout the force. To follow, establish a new Universal Joint Task List (UJTL) task across all joint functions at the Operational (OP) and Tactical (TA) levels: "perform effective [function] in a degraded or denied communications environment (D2CE)."

SELECTED BIBLIOGRAPHY

Berg, Paul D., U.S.A.F. "Expeditionary Operations." *Air & Space Power Journal* 22, no. 2 (Summer, 2008). http://search.proquest.com/docview/217769894?accountid=322. Accessed April 12, 2014.

Cliff, Roger, Mark Burles, Michael S. Chase, Derek Eaton, and Kevin L. Pollpeter. *Entering the Dragon's Lair.* Santa Monica, CA: The RAND Corporation, 2007.

Dai, Qingmin. "On Integrating Network Warfare and Electronic Warfare." *Zhongguo Junshi Kexue*, 1 February, 2002. In *FBIS [Foreign Broadcast Information Service] as "Chinese Military's Senior EW Official Explains China's Network Warfare Doctrine."* June 24, 2002.

Drew, James. "House Subcommittee Hears of Chinese Threats to U.S. Space Assets." *Inside the Pentagon's Inside Missile Defense* vol. 20, no. 3 (Feb 05, 2014), http://search.proquest.com/docview/1494380793?accountid=322. Accessed April 10, 2014.

Everstine, Brian. "Pilots Shut Off GPS, Other Tools to Train for Future Wars." *Air Force Times*, no. 23 (Oct 21, 2013). http://search.proquest.com/docview/1460871673?accountid=322. Accessed April 10, 2014.

Freedberg Jr, Sydney J. "Air Force Seeks Quick Fixes to Combat Chinese Electronic Attacks." *Breaking Defense*, September 18, 2012. http://breakingdefense.com/2012/09/air-force-seeks-quick-fixes-to-combat-chinese-electronic-attacks/.

Gordon, John IV and John Matsumara. *The Army's Role in Overcoming Anti-Access and Area Denial Challenges.* Santa Monica, CA: The RAND Corporation, 2013.

Howe, Neil and William Strauss. *Millennials Rising: the Next Great Generation.* New York, NY: Vintage Books, 2000.

Fitzgerald, David. *Learning to Forget: US Army Counterinsurgency Doctrine and Practice from Vietnam to Iraq*. Stanford, CA: Stanford University Press, 2013.

Johnston, Paul. "Doctrine is Not Enough: The Effect of Doctrine on the Behavior of Armies." *Parameters* 30, no. 3 (Autumn, 2000).

Lagrone, Sam. "Pentagon's 'Air-Sea Battle' Plan Explained – Finally". *Wired,* 6 August 2012. http://www.wired.com/2012/08/air-sea-battle-2/.

Lanham, Michael J. "When the Network Dies." *Armed Forces Journal,* no. 10 (Dec 01, 2012). http://search.proquest.com/docview/1285153378?accountid=322. Accessed April 10, 2014.

Lu, Daohai. *Information Operations: Exploring the Seizure of Information Control.* Beijing, People's Republic of China: Junshi Yiwen Press, 1999.

Magnuson, Stew. "U.S. Forces Prepare For a Day Without Space." *National Defense Magazine,* February 2014. http://www.nationaldefensemagazine.org/archive/2014/February/pages/USForcesPreparefora%E2%80%98DayWithoutSpace%E2%80%99.aspx

Meteyer, David O. *The Art of Peace: Dissuading China from Developing Counter-Space Weapons.* INSS Occasional Paper 60. Colorado Springs, CO: USAF Institute for National Security Studies, 2005.

Office of the Director of National Intelligence. *Worldwide Threat Assessment of the U.S. Intelligence Community.* Tyson's Corner, VA: Office of the Director of National Intelligence, January 2014. http://www.dni.gov/index.php/newsroom/testimonies/203-congressional-testimonies-2014/1008-remarks-as-delivered-by-dni-james-r-clapper-on-the-2014-world-wide-threat-assessment?tmpl=component&format=pdf. Accessed April 10, 2014.

Podvig, Pavel and Hui Zhang. *Russian and Chinese Responses to U.S. Military Plans in Space*. Cambridge, MA: The American Academy of Arts and Sciences, 2008.

Rickards, David A. "No Air: Cyber Dependency and the Doctrine Gap". Research Paper, U.S. Naval War College, Joint Military Operations Department, Newport, RI, 2010.

Tirpak, John A. "Gates Versus the Air Force." *Air Force Magazine*. Vol. 97, No. 3 (2014). http://www.airforcemag.com/Features/Pages/2014/box020514gates.aspx.

van Tol, Jan, Mark Gunzinger, Andrew Krepinevich, and Jim Thomas. *AirSea Battle: A Point-of Departure Operational Concept.* Washington, DC: Center for Strategic and Budgetary Assessments, 2010.

U.S. Department of Defense. *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense.* Arlington, VA: Department of Defense, January 2012.

U.S. Department of Defense. *Joint Operational Access Concept, Version 1.0.* Arlington, VA: Department of Defense, January 2012.

U.S. Federal News Service, LLC. "Navy Warfare Development Command Releases Tactical Memorandum." *US Fed News Service, Including US State News,* Jun 12, 2012, http://search.proquest.com/docview/1019843532?accountid=322 (accessed April 15, 2014).

U.S. Naval War College. Briefing. Subject: Global 2013 Game Report, 11 March 2014.

U.S. Office of the Chief of Naval Operations. *Required Operational Capabilities and Projected Operational Environment for Amphibious Command Ship (LCC-19) Blue Ridge.* OPNAV Instruction 3501.33F. Washington D.C.: DON, 8 May 2013.

Waghelstein, John D. "Military-to-Military Contacts: Personal Observations – The El Salvador Case" (Fall 2002). Quoted in Frank Cass, *Low Intensity Conflict and Law Enforcement*, London Vol. 10, No2, Summer 2003.

Wolthusen, Stephen D., "Self-Inflicted Vulnerabilities," *Naval War College Review*, Vol. LVII, Nos. 3–4 (2004).

Yoshihara, Toshi and James R. Holmes. *Red Star Over the Pacific.* Annapolis, MD: Naval Institute Press, 2010.